Part I
Grundlagen

1 Verbände

Definition 0.1. Die Kategorie der Verbände

2 Kategorien

In diesem Abschnitt werden die nötigen kategorientheoretischen Kenntnisse (bzw. Terminologie) bereitgestellt, welche für die Gruppentheorie (von einem modernen Standpunkt aus) unentbehrlich sind.

1 Terminale und finale Objekte

Definition 0.2 (initiale und terminale Objekte). Sei $\boldsymbol{A}$ eine Kategorie. Dann heißt ein Objekt $T : \boldsymbol{A}$ *terminal*[1], falls es für jedes andere Objekt $O : \boldsymbol{A}$ genau einen Morphismus $\alpha : O \to T$ gibt. Mit anderen Worten: T ist maximal bezüglich der transitiven Relation $\to$. In analoger Weise heißt I ein *initiales*[2], falls es für jedes $O : \boldsymbol{A}$ genau einen Morphismus $\beta : I \to O$ gibt. Mit anderen Worten: I ist minimal bezüglich der transitiven Relation $\to$.

Definition 0.3 (Nullobjekt). Ein Objekt $0 : \boldsymbol{A}$ heißt *Nullobjekt*[3], falls 0 sowohl initial als auch terminal ist.

2 Initiale und terminale Pfeile und Nullpfeile

Definition 0.4 (Initiale und terminale Pfeile). Ein Pfeil $\gamma : A \to B$ heißt *terminaler Morphismus*[4], falls $\alpha\gamma = \beta\gamma$ für alle $\alpha, \beta :\to A$. Analog heißt γ *initialer Morphismus*[5], falls $\gamma\alpha = \gamma\beta$ für $\alpha, \beta : B \to$ (d.h. γ^* ist konstant in $\boldsymbol{A}^*$).

Bemerkung 1. Initiale und terminale Pfeile sind genau die initialen und terminalen Objekte in der Morphismenkategorie von $\boldsymbol{A}$.

Definition 0.5 (Nullpfeil). Ein Pfeil $0 : A \to B$ heißt *Nullmorphismus*[6], falls er konstant und kokonstant zugleich ist.

Bemerkung 2. Nullpfeile sind genau die Nullobjekte in der Morphismenkategorie von $\boldsymbol{A}$.

[1] terminales Objektkoinitiales Objekt
[2] initiales Objektkoterminales Objekt
[3] Nullobjekt
[4] terminaler Morphismuskonstanter Morphismus
[5] initialer Morphismuskokonstanter Morphismus
[6] Nullmorphismus

Bemerkung 3. Gibt es ein Nullobjekt $0 : \boldsymbol{A}$, so auch ein kanonischen Nullmorphismus zwischen Objekten $A, B : \boldsymbol{A}$ via $A \to 0 \to B$, wobei die beiden Morphismen aufgrund der Nullobjekteigenschaft schon eindeutig sind.

3 Kerne und Kokerne

Definition 0.6 (Kern und Kokern). Sei $\alpha : A \to_{\boldsymbol{A}} B$ ein Morphismus. Dann wird ist der *Kern*[7] $\ker \phi$ das Unterobjekt mit der universellen Eigenschaft, dass jedes Unterobjekt U von A gilt, dass $U\alpha = 0_{\mathrm{Sub}\, A}$, dann gilt $\ker \phi \leq U$. In analoger Weise definieren wir den *Kokern*[8] $\ker^* \alpha$ von α als das Quotientenbojekt Q von B, welches die Eigenschaft hat, dass $\alpha Q = 0_{\mathrm{Sub}^* A}$ gilt $\ker^* \alpha \leq Q$.

4 Unterobjekte und Quotientenobjekte

Definition 0.7. Sei $\boldsymbol{A}$ eine Kategorie. Der Verband der *Unterobjekte*[9] $\mathrm{Sub}\, A$ für jedes Objekt $A : \boldsymbol{A}$ als die Isomorphieklassen der Kategorie $\rightarrowtail_{\boldsymbol{A}} A$ (also $\rightarrowtail_{\boldsymbol{A}} A / \leftrightarrow$). Analog definieren wir den Verband der *Quotientenobjekte*[10] von A als $\mathrm{Sub}^* A$ durch die Isomorphieklassen von $A \twoheadrightarrow_{\boldsymbol{A}} / \leftrightarrow$.

Bemerkung 4. Die beiden Konzepte sind also genau dual zueinander.

5 Normale Unterobjekte und konormale Quotientenobjekte

Definition 0.8 (Normales Unterobjekt und konormales Quotientenobjekt). Ein Unterobjekt N von A heißt *normal*[11], falls es einen Morphismus $\alpha : A \to$ gibt, sodass $N = \ker \alpha$. Ein Quotientenobjekt Q heißt *konormal*[12], falls es einen Morphismus $\beta :\to \alpha$ gibt mit $\ker^* \beta = Q$.

6 Bilder

Definition 0.9. Sei $\alpha : A \to B$ ein Morphismus, dann bezeichnet *image*α das induzierte Unterobjekt von α.

7 Normale Morphismen

Definition 0.10. Ein Morphismus $\alpha : A {\to}_{\boldsymbol{A}} B$ heißt *normal*[13], falls $\mathrm{im}\, \alpha$ ein normales Unterobjekt von B ist.

[7] Kern eines Morphismus
[8] Kokern
[9] Unterobjekt
[10] QuotientenobjektKounterobjekt
[11] normales Unterobjekt
[12] konormales Quotientenobjekt
[13] normaler Morphismus

8 Morphiesätze

Satz 0.1. *Sei $\boldsymbol{A}$ eine Kategorie mit Bildern und Kernen. Sei $\phi : A \to_{\boldsymbol{A}} B$ ein Morphismus. Dann gibt es ein Objekt C mit $\pi : A \twoheadrightarrow C$, $\iota : C \rightarrowtail B$, sodass $\phi = \pi\iota$.*

Beweis. ∎

3 Produkte und Koprodukte

Sei $\boldsymbol{B} \rightarrowtail \boldsymbol{A}$ eine Unterkategorie.

4 Gruppenaxiome

Unter einer Gruppe verstehen wir eine Struktur vom Typ $\boldsymbol{Grp} = \left\langle \circ, ^{-1}, 1 \right\rangle$, derart dass folgende Identitäten gelten

- $(a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativität)
- $a^{-1} \circ a = a \circ a^{-1} = 1$ (Inversenabblildung)
- $a \circ 1 = 1 \circ a = a$ (neutrales Element)

Satz 0.2. *Hallo*

5 Aufsteigende und absteigende Kettenbedingung

Definition 0.11. Sei P : $\boldsymbol{Poset}$. Dann genügt P der *aufsteigenden Kettenbedingung*[14], wenn jede aufsteigende Kette nach endlich vielen Gliedern abbricht. Analog genügt P der *absteigenden Kettenbedingung*[15]

Satz 0.3 (Charakterisierung von endlicher Erzeugbarkeit). *Sei A eine Algebra. Die folgenden Aussagen sind äquivalent*

(I) *A ist endlich erzeugt.*

(II) $\operatorname{Sub} A$ *genügt der aufsteigenden Kettenbedingung.*

(III) *Jedes Unterobjekt U : $\operatorname{Sub} A$, $U \neq A$ liegt in einem maximalen Unterobjekt.*

Beweis.

Ist A endlich erzeugt und C eine aufsteigende Kette in $\operatorname{Sub} A$, dann wird C stationär.

[14] aufsteigende KettenbedingungNoether'sche Eigenschaft
[15] absteigende KettenbedingungArtin'sche Eigenschaft

blub

∎

6 Die Sylow'schnen Sätze

Eine natürliche Frage, welche sich aus dem Theorem von Lagrange ergibt, welche Aussagen über die Anzahl und Art der Untergruppen von Ordnung n einer endlichen Gruppe G getroffen werden können. Für $n \nmid |G|$ ist selbige Anzahl nach dem Theorem von Lagrange (TODO: REF) gleich null. Ist G zyklisch, so ist jene Anzahl im Falle $n \mid |G|$ genau eins. Tatsächlich muss es aber für $n \mid |G|$ keine Untergruppen dieser Ordnung geben, was man am leichtesten an der symmetrischen Gruppe $\operatorname{Aut} m$ sieht, denn wählt man nun n als eine Zyklizität erzwingende Zahl, sodass $m < n|m!$, dann gibt es offensichtlich keine Untergruppen von $\operatorname{Aut} m$ dieser Ordnung. ist es ob bei einer endlichen Gruppe G der

Tatsächlich lassen sich aber befriedigende Aussagen treffen, falls $n = p^e$ die Potenz einer Primzahl p ist. Diese werden gemeinhin als Sylow'sche Sätze bezeichnet.

Definition 0.12 (p-Gruppe). Sei G eine Gruppe derart, dass jedes Element $g \in G$ eine Primzahlpotenz p^{e_g} als Ordnung hat (wobei p eine feste Primzahl sei.

Bemerkung 1. Eine triviale Konsequenz der Sylow'schen Theoreme wird es sein, dass jede endliche p-Gruppe selbst von Primzahlpotenzordnung p^e ist.

Satz 0.4 (Existenz von p-Untergruppen jeder Ordnung). *Sei G eine endliche Gruppe mit $|G| = p^e n$. Für die Anzahl $N_{p^e} := |\langle U \leq G : |U| = p^e \in \mathrm{Set}\rangle|$ gilt dann*

$$N_{p^e} = 1 \; mod \; p$$

Beweis. Wir betrachten die Aktion von G auf den p^e-elementigen Untermengen von G_{Set} welche gegeben wird durch elementweise Rechtsmultiplikation. Die Bahnengleichung für diese Aktion wird dann zu

$$\left|\begin{pmatrix} G_{\mathrm{Set}} \\ p^e \end{pmatrix}\right| = \sum_i \left|G/\mathrm{stab} A_i\right|,$$

wobei A_i Repräsentanten der G-Bahnen sind. Für $A_i \rightarrowtail G_{\mathrm{Set}}$, $|A_i| = p^e$ gilt allerdings dann $A_i(\mathrm{stab} A_i)_{\mathrm{Set}} = A_i$, also ist A_i eine disjunkte Vereinigung von Linksnebenklassen von $\mathrm{stab} A_i$ und mithin $|\mathrm{stab} A_i| \mid p^e$. Betrachten wir also obige gleichung modulo pn, so folgt

$$\begin{pmatrix} p^e n \\ p^e \end{pmatrix} = nN_{p^e} \bmod pn,$$

denn alle Terme, in denen $\mathrm{stab} A_i < p^e$ ist in obiger Gleichung entfallen und die übrigen Terme zählen genau für jede p^e-elementige Untergruppe von G ihre Linksnebenklassen (derer gibt es n). Daraus folgt

$$\frac{1}{n}\binom{p^e n}{p^e} = \binom{p^e n - 1}{p^e - 1} = N_{p^e} \bmod p,$$

wobei der Ausdruck auf der Linken Seite gleich 1 ist modulo p. Dies sieht man einerseits daran, dass dies für die zyklische Gruppe mit $p^e n$ Elementen gilt, andererseits lässt sich auch das Theorem von Lucas (TODO : REF) auf den letzten Binomialkoeffizienten anwenden. Wir erhalten dann

$$N_{p^e} = \binom{p^e n - 1}{p^e - 1} = \binom{p-1}{p-1}^e = 1 \bmod p.$$

■

Text

Satz 0.5. *Jede endliche Gruppe G hat p-Sylow-Gruppen. Für jede p-Untergruppe U und eine p-Sylow-Gruppe von G gibt es ein Element $g \in G$, sodass $U \rightarrowtail P^g$. Insbesondere sind alle p-Sylow-Gruppen konjugiert zueinander und ihre Anzahl ist $|G/N_G P|$.*

7 Die Sätze von Hall

Die Sätze von Hall stellen eine Verallgemeinerung der Sylow'schen Sätze für auflösbare Gruppen dar. Entsprechende Untergruppen nennt man auch Hall-Untergruppen.

Satz 0.6 (Hall'sches Theorem). *Sei G auflösbar und $|G| = mn$ mit teilerfremden m und n. Dann gilt*

(I) Sei U eine Untergruppe mit $|U|\,|m$ und M eine Untergruppe der Ordnung m, dann gibt es ein $g \in G$ sodass $U \leq M^g$.

(II) Für die Anzahl der Untergruppen der Ordnung m von G gilt:

$$N_m = 1 \; mod \; \mathrm{rad} m$$

Beweis. Der Beweis erfolgt per Induktion nach der Anzahl k der Primfaktoren von m. Für $k = 1$ gilt die Aussage schlicht aufgrund der Sylow'schen Sätze auch ohne Auflösbarkeit von G.

■

Satz 0.7 (Frattini-Argument). *Sie G eine Gruppe und $N \leq_{\mathrm{Con}\, G} G$. Weiter sei P eine Untergruppe von N derart, dass alle zu P isomorphen Untergruppen in H konjugiert sind (also z.B. P eine p-Sylow-Gruppe). Dann gilt $G = \mathrm{N}_G PN$.*

Beweis. Für $g \in G$ ist P^g isomorph zu P und gleichermaßen Untergruppe von N, da N normal in G liegt. Also sind P und P^g in N konjugiert und es folgt $P^{gn} = P$ für geignetes $n \in N$. Damit ist aber $gn \in \mathrm{N}_G P$ und somit auch $g \in N\mathrm{N}_G P$. ∎

8 Auflösbarkeit von Gruppen

Definition 0.13 (Subnormalenverband, Subnormalenreihe). Ein Unterverband $\boldsymbol{U}$ von $\operatorname{Sub} G$ Subnormalenverband, falls für alle $U \in \boldsymbol{U}$ gilt $U \in \operatorname{Con} \bigwedge_{V>U} V$. Ist ein solcher Verband isomorph zu einem Unterverband von $\mathbb{N}_{\mathrm{Lat}}$, so nennen wir Ihn eine Subnormalenreihe.

Definition 0.14 (Auflösbare Gruppe). Eine Gruppe G heißt *auflösbar*[16], falls es einen Subnormalenverband von G gibt, derart, dass

$$\bigwedge_{V>U} V/U \text{ kommutativ}$$

für alle $U \in U$. *endlich auflösbar*[17][18]

Definition 0.15 (Kommutatoruntergruppe). Seien $\boldsymbol{U} \leq \operatorname{Sub} G_{\mathrm{Set}}$. Dann bezeichnen wir mit $[\boldsymbol{A}]$ die *Kommutatoruntergruppe*[19] von der Gruppen in $\boldsymbol{A}$. Sie wird erzeugt durch alle Kommutatoren $[a, b]$ für $a \in A, b \in B, A, B \in \boldsymbol{A}$.

Lemma 0.1. *Die Kommutatoruntergruppe $[\boldsymbol{A}]$ ist charakterisiert durch folgende univerelle Eigenschaft. Sei N ein Normalteiler von $\langle \boldsymbol{A} \rangle$ derart, dass unter der kanonischen Projektion $\pi : \langle \boldsymbol{A} \rangle \to \langle \boldsymbol{A} \rangle / N$ die Bilder der Elemente von $\boldsymbol{A}$ paarweise elementweise kommutieren, d.h. $[\operatorname{im} \iota_A \pi, \operatorname{im} \iota_B \pi] = 1$, wobei ι_A bzw. ι_B die Inklusionen von Untergruppen $A, B \in \boldsymbol{A}$ sind, dann ist $[\boldsymbol{A}] \leq N$ und in äquivalenterweise gibt es einen eindeutigen Morphismus π', sodass $\pi = p\pi'$ mit $p : \langle \boldsymbol{A} \rangle \to \langle \boldsymbol{A} \rangle / N$ die kanonische Abbildung.*

Beweis. Der Beweis folgt aus dem allgemeineren Kontext (TODO). ∎

Definition 0.16 (Kommutatorreihe). Wir definieren die *Kommutatorreihe*[20] $\left(G^{(i)}\right)_{i \in \mathbb{N}}$ einer Gruppe G als

$$G^{(0)} := G,\ G^{(i+1)} := \left[G^{(i)}, G^{(i)}\right] \ (i \in \mathbb{N}).$$

Weiterhin setzen wir $G^{(\omega)} := \bigwedge_{i \in \mathbb{N}} G^{(i)}$ und bezeichnen es als *perfekten Kern*[21] von G.

[16] auflösbare Gruppe
[17] endliche auflösbare Gruppe
[18] Dies meint auflösbar im herkömmlichen Sinne.
[19] Kommutatorgruppe
[20] Kommutatorreihe
[21] perfekter Kern

Lemma 0.2. *Eine Gruppe G ist genau dann endlich auflösbar, falls ihre Kommutatorreihe nach endlich vielen Schritten in 1 endet. Sie ist genau dann ω-auflösbar, falls ihr perfekter Kern gleich 1 ist.*

Beweis. Sei $\boldsymbol{G}$ ∎

9 Der Satz von Jordan-Hölder

9 Das Zassenhaus-Theorem (Schmetterlings-Theorem)

Satz 0.8 (Schmetterlingslemma). *Sei $A \leq_{\mathrm{Con}\,G} B$ und $C \leq_{\mathrm{Con}\,G} D$, dann gilt*

$$\frac{(B \wedge D) \vee A}{(B \wedge C) \vee A \leftrightarrow (B \wedge D)(B \wedge C) \vee (A \wedge D) \leftrightarrow (B \wedge D) \vee C(A \wedge D) \vee C.}$$

Beweis. ∎

$$\begin{tikzcd}
A \arrow[r, "\phi\quad\psi"] \arrow[d] & B \arrow[d, "\xi", color=red] \\
C \arrow[r, "\eta", color=red] & D
\end{tikzcd}$$

$\mathcal{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$abcdefghijklnmopqrstuvwxyz$
$\mathfrak{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$\mathfrak{abcdefghijklnmopqrstuvwxyz}$
$\boldsymbol{ABCDEFGHIJKLNMOPQRSTUVWXYZ}$
$\boldsymbol{abcdefghijklnmopqrstuvwxyz}$
$\rightarrow \rightarrowtail \twoheadrightarrow$